Time stamping data with official time e.g. for electronic signature on digital documents by using decrypted official time signal to set internal time source

Patent number:	DE19845199
Publication date:	2000-04-06
Inventor:	BECKER BERND (DE); FISCHER FRANK (DE)
Applicant:	MAZ MIKROELEKTRONIK ANWENDUNGS (DE)
Classification:	
- international:	H04Q7/06; H04L9/00; G04C11/02; G04G7/02; G06F1/14
- european:	H04L9/32S
Application number:	DE19981045199 19981001
Priority number(s):	DE19981045199 19981001

Abstract of **DE19845199**

The method involves supplying a local and/or global official time signal to a mobile network operator (e.g. GSM). The time is encrypted and decrypted based on the technology of the network operator before being transmitted to the customer. The decrypted official time signal is used to set an internal time source. Digital data are time-stamped with this official time signal. The time-stamped data are encrypted and provided with a digital signature.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 45 199 A 1**

(21) Aktenzeichen: 198 45 199.7
(22) Anmeldetag: 1. 10. 1998
(43) Offenlegungstag: 6. 4. 2000

(51) Int. Cl.[7]:
H 04 Q 7/06
H 04 L 9/00
G 04 C 11/02
G 04 G 7/02
G 06 F 1/14

DE 198 45 199 A 1

(71) Anmelder:
MAZ Mikroelektronik Anwendungszentrum Hamburg GmbH, 21079 Hamburg, DE

(74) Vertreter:
Diehl, Glaeser, Hiltl & Partner, 22767 Hamburg

(72) Erfinder:
Becker, Bernd, 21079 Hamburg, DE; Fischer, Frank, 21261 Welle, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

GB	21 94 416 A
EP	08 83 314 A2
WO	96 41 488 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zur Zeitstempelung von Daten mit der amtlichen Zeit

(57) Die Erfindung bezieht sich auf ein Verfahren zur Zeitstempelung von Daten mit der amtlichen Zeit mit folgenden Verfahrensstufen:
Einspeisung der Zeitinformationen (Datum, Uhrzeit, lokal oder global) in die Netze (GSM, UMTS) der Mobilnetzbetreiber,
Verschlüsselung der Zeitinformationen,
Übergabe der verschlüsselten Zeitinformationen an mindestens ein Endgerät (mobile und/oder fest installierte Endgeräte) des jeweiligen Endgerätebetreibers,
Entschlüsselung der Zeitinformationen im Endgerät, so dass ab Verschlüsselung und bis Entschlüsselung, jeweils basierend auf der Technologie des Netzbetreibers, die Zeitinformationen manipulationssicher übertragen werden, und
Nutzung der entschlüsselten Zeitinformationen zum Stellen einer Zeitquelle im Endgerät zwecks Zeitstempelung digitaler Datensätze mit diesen Zeitinformationen und Signatur der zeitgestempelten digitalen Datensätze.

DE 198 45 199 A 1

Beschreibung

Hinweise

Der Patentanspruch ist explizit formuliert, um die Erfindung von den Komponenten eines Gesamtsystems in diesen Anwendungsfällen abzugrenzen.

Zweck des Dokuments

Dies Dokument beschreibt eine neue Methode und die daraus folgenden technischen Lösungen zur Zeitstempelung mittels einer manipulationssicheren, amtlichen Zeit, wie sie der Gesetzgeber im Zeitgesetz vom 25.07.1978, dargestellt im Bundesgesetzblatt Teil 1 S. 1110–1111, zum amtlichen und geschäftlichen Verkehr fordert.

Das Dokument bildet die Basis zur Ausarbeitung eines Patentes, um die hier beschriebene Erfindung zu schützen.

Einleitung

Durch die Zunahme an elektronischer Kommunikation wird der Schutz der zu übertragenen Daten immer wichtiger. In der elektronischen Datenkommunikation ist es von Bedeutung, die Vorlage von elektronischen Daten zu einem bestimmten Zeitpunkt nachweisen zu können.

Die nachfolgend beschriebene Erfindung ermöglicht die Zeitstempelung digitaler Daten mit einer manipulationssicheren, amtlichen Zeit.

Detaillierte Beschreibung

Anwendungsbereiche der Erfindung

Für die Beweiskraft elektronischer Dokumente müssen der Autor, die Zeit und der Ort der Unterzeichnung manipulationssicher festgehalten und nachgeprüft werden können. Zu diesem Zweck empfiehlt der Gesetzgeber "Digitale Signaturen", welche die Unverschrtheit und die Authentizität der Daten sicherstellen. Um die Vorgaben des Signaturgesetzes umsetzen zu können, müssen mehrere technische Probleme gelöst werden, eines ist die Verwendung einer manipulationssicheren, amtlichen Zeit. Dies ist in besonderem Maße von Bedeutung, da die asymmetrischen Algorithmen zur digitalen Signatur nur durch das Hinzufügen einer nicht manipulierbaren Zeitinformation die Anforderungen an die Fälschungssicherheit von Signaturen oder signierten Daten gewährleistet werden kann.

Neben der Signatur ist eine genaue manipulationssichere Zeit aber auch für andere technische Komponenten wie z. B. Rechnersysteme von Bedeutung.

Technische Grundlagen

Zu Grunde gelegt werden amtliche Zeitsignale, wie sie auf nationaler oder aber auch auf internationaler Ebene zur Verfügung gestellt werden.

Ähnlich dem deutschen DCF77 Zeitsignals erzeugen auch Großbritanien und Frankreich ihr eigenes amtliches Zeitsignal.

Als Punkt zu Punkt Verbindung einer drahtlosen Übertragungs-Technologie wird das weit verbreitet GSM-Netz zu Grunde gelegt.

Der Signatur werden keine konkreten Verfahren zugeordnet, da dieser Markt noch stark in Bewegung ist, und derweil noch keine Endgültige Tendenz aufweist.

DCF77-Signal

Das nationale deutsche amtliche Zeitsignal DCF77 wird von der PTB (Pysikalische Technische Bundesanstalt) in Braunschweig ausgestrahlt.

Dieses abgestrahlte Zeitsignal, bei einer Frequenz von 77,5 kHz (amplitudenmoduliert), besitzt allerdings eine eingeschränkte Reichweite von bis zu 2000 km. Dieses bedeutet, daß ein europäisches Zeitsignal flächendeckend nicht vorhanden ist.

Weitere Einschränkungen treten am Empfänger auf, da auf Grund der langen Wellenlänge schon die nächste Umgebung als empfangsstörend wirken kann.

Weiterhin ist es möglich durch den Nachbau eines manipulierten DCF77 Senders, diesen als "quasi amtliches Zeitsignal" zu verwenden. Um die korrekte Verwendung eines amtlichen Zeitsignals zu gewährleisten, ist es demnach zwangsläufig notwendig, dieses Signal nicht nur beim Endanwender zu schützen, sondern schon während der Übertragung zum Anwender durch geeignete Verfahren. An dieser Stelle kommt eine Verschlüsselungsverfahren zum Einsatz, wie es im nachfolgenden Abschnitt beschrieben wird.

GSM als Übertragungstechnologie

Die Verwendung von GSM als Basis zur drahtlosen Punkt zur Punkt Übertragung findet nicht nur bei der Telekommunikation ein weites Anwendungsfeld. So sind die Betreiber dieser GSM Netze darauf bedacht, immer neue Anwendungsmöglichkeiten dem Endverbraucher zur Verfügung zu stellen. Dieses ist in den zurückliegenden Jahren mit der Abfrage von Wetterdaten, Fußballergebnissen, Börsenständen, aktuellen Nachrichten, usw. mit einem "Short Message Service

(SMS)" durchgeführt worden.

Die Übertragung dieser SMS's erfolgen verschlüsselt und sind damit ausschließlich dem Endanwender, der dafür eine Gebühr an den Provider entrichtet, zugänglich.

Die Übetragungsfrequenzen liegen in zwei Frequenzbändern bei 900 MHz und 1,8 GHz.

Signatur

Der Gesetzgeber fordert neben der Personenbezogenen Signatur von Daten gleichzeitig den Zeitpunkt und weitere Angaben dieser Signierung. Der Maßnahmenkatalog für digitale Signaturen, auf Grundlage des SigG und der SigV Kapitel 6.5.4.2.2 und 6.5.4.2.3, M-TSS6 bis M-TSS14 sieht dafür nachfolgende Angaben vor.

In einer für die Durchführung der Signatur vorgesehene Sicherheitsbox werden die digitalen Daten um die aktuelle Zeit (Tag, Monat, Jahr, Stunden Minuten, ggf. Sekunden und Zeitzone) ergänzt.

Zusätzlich werden in einem Protokoll mindestens folgende Angaben protokolliert:
$Signatur_{TSS}$ ($Hash_{(Daten,Zeit)}$), die Zeit und die laufende Nr. des Zeitstempels.

An dieser Stelle ist zu berücksichtigen, daß der Gesetzgeber eine gesetzliche anerkannte Zeit, wie das DCF77-Signal in Deutschland, fordert.

Technische Beschreibung

Die im Kapitel 4.2 verwendeten Standards werden nun als Verfahren zur Übermittlung einer manipulationssicheren, amtlichen Zeit mit Hilfe eines Verschlüsselungsverfahren, wie es bei Mobil-Netzbetreibern (z. B. GSM) zum Einsatz kommt, zusammengefügt. Des Weiteren wird diese amtliche Zeit durch stellen einer internen Zeitquelle Grundlage zum amtlichen Zeitstempel und damit zur digitalen Signatur.

Voraussetzungen

Der Endanwender muß sich im Vorfeld den Übermittlungs-Dienst des Providers sichern. Des Weiteren muß der Endanwender die technische Möglichkeit der Auswertung der übertragenen Daten besitzen. Weiterhin muß eine Vorrichtung zur Weiterverarbeitung des Zeitsignals, zur Verschlüsselung und zur Signatur der digitalen Daten vorhanden sein.

Realisierung

Das von der PTB in Braunschweig ausgehende Zeitsignal wird von einem GSM-Netzbetreiber aufgegriffen. Der GSM-Netzbetreiber verschlüsselt nun die Zeitangabe aus diesem Signal und übermittelt sie dem Endanwender. (kontinuierlich oder auf Anforderung).

Die Entschlüsselung des Datenstrings nach dem Empfang geschieht in einer physikalisch und logisch gesicherten "Box" (Sicherheitsbox).

Im Anschluß daran steht die übertragene, amtliche Zeit in ursprünglicher Form zur Verfügung. Mit dieser nun vorliegenden amtlichen Zeit wird eine "Box-interne" Hardware-Uhr mit der amtlichen Zeit neu gestellt.

Nun ist der Endanwender in der Lage, sofort nach Abschluß der vorangegangenen Prozedur die Zeitstempelung der digital erzeugten Daten mit der amtlichen Zeit durchzuführen und seine Daten zu signieren.

Vorteile des Verschlüsselungsverfahrens der amtlichen Zeit

Durch das Verschlüsselungsverfahren der amtlichen Zeit wird sichergestellt, daß eine Manipulation auf dem Übertragungsweg zwischen der DCF77 Signalquelle und dem Empfangsmodul des Endanwenders ausgeschlossen wird.

Der GSM-Netzbetreiber hat ebenfalls Vorkehrungen diesbezüglich zu treffen.

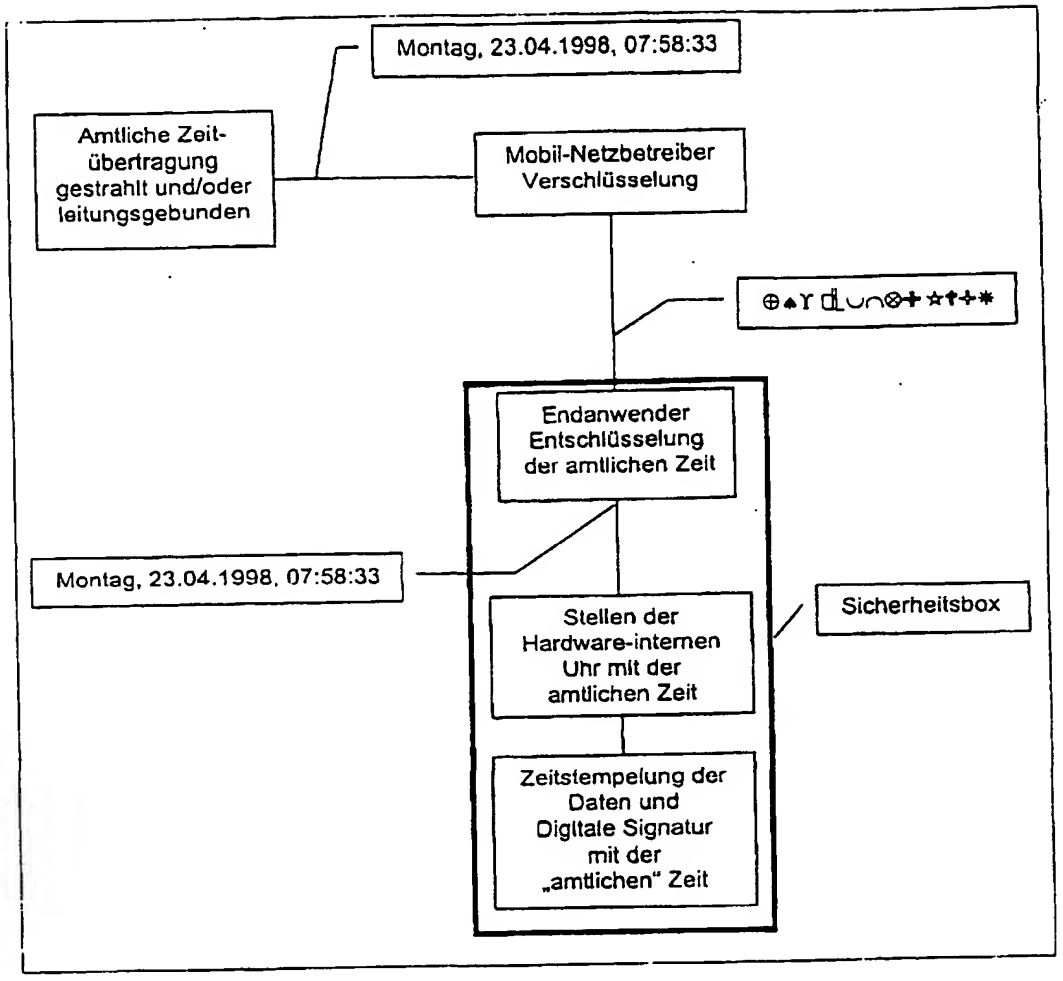
Die Manipulationssicherheit:

a) des Zeitsignals nach der Entschlüsselung beim Empfänger,
b) das Stellen der Hardware-internen Uhr und
c) die Durchführung der vollständigen digitalen Signatur

werden anderweitig physikalisch und logisch in der Sicherheitsbox realisiert.

Die nachfolgende Abbildung stellt die im Abschritt: "Realisierung" beschriebene Vorgehensweise grafisch dar.

Abbildung: Schematischer Aufbau



Anwendungsbeispiel

Als möglicher Dienstleistungsanbieter dieses Short Message Services, bietet sich die Telekom an, da diese sowohl als Betreiber eines GSM-Netztes auftritt, als auch indirekt an dem Betrieb des DCF77-Signals beteiligt ist.

Patentansprüche

Verfahren zur Zeitstempelung von Daten mit der amtlichen Zeit mit folgenden Verfahrensstufen:

- Einspeisung eines lokalen und/oder globalen amtlichen Zeitsignals in die Übertragungstechnologie eines Mobil-Netzbetreibers,
- Verschlüsselung und Entschlüsselung der Zeit, basierend auf der Technologie des Netzbetreibers mit anschließender Übergabe an den Kunden,
- Nutzung des entschlüsselten, amtlichen Zeitsignals zum Stellen einer internen Zeitquelle,
- Zeitstempelung digitaler Daten mit diesem "amtlichen" Zeitsignal und
- Verschlüsselung und Signatur der zeitgestempelten digitalen Daten.